Search the SafetyCulture blog

Ask The Experts | Customer Stories | Industry Trends | Media Release | Moments That Matter | SafetyCulture News | World Of Work

‹ Back to home page

What manufacturing workers need to know about cybersecurity

Industry Trends | By **SafetyCulture Team** | 2 Feb 2024 | 4 minute read

When it comes to safeguarding cybersecurity, workers are a facility's first line of defense. SafetyCulture works with manufacturing teams day in and day out, and we know this is something every business is grappling with. If you know the biggest threats and how to deal with them, you can protect your workplace.

The biggest cybersecurity risks manufacturers face

Hackers often focus on manufacturing because it's fundamental to many other industries. Lately, they've been targeting workers to increase their chances of success. Here are the biggest cybersecurity risks manufacturers face.

Credential stuffing

Credential stuffing is a brute-force attack where hackers use stolen login details to get into a system they shouldn't have authorized access to. It was one of the most common cyber attacks in 2023 because of its subtle nature.

Supply chain attacks

A good chunk of SafetyCulture's customers work with supply chains. Marley Spoon, for example, deals with producers to supply their fresh produce, which makes up the ingredients for their recipes, which are then distributed to their customers.

A supply chain cyber attack targets third-party vendors. Hackers go through them to gain access to a facility's data, network, or systems. Computer manufacturer ASUS experienced this firsthand. Hackers stole their vendors' authentication keys to remotely send malicious updates for five months – impacting at least one million people – before being caught.

Phishing

If you've received an odd email or SMS with a shady-looking attachment, it was probably a phishing attempt – where someone sends a malicious link to download malware or steal information. "Be vigilant when receiving SMS messages or emails out of the blue," says Steven Rogers, Cybersecurity Group Engineering Manager at SafetyCulture. "Always check carefully any links you intend to click to make sure they are taking you to the legitimate website. Call the company or ask friends to confirm."

Ransomware

Once cybercriminals encrypt company data or lock its systems, they can demand millions of dollars to return access. Usually, they can get in using malicious links. In 2023, car manufacturer Nissan had to shut down operations in Australia and New

Zealand for a month because of a ransomware attack. If you find yourself under a ransomware attack, “turn off your device and seek specialist guidance before the problem becomes bigger,” Steve advises.

Internal breaches

Believe it or not, employees are a common cause of data breaches. Incorrectly updated factory floor equipment and malware-downloading misclicks are common. Considering a single incident costs more than $4.24 million on average, you have great motivation to stay proactive.

> **Did you know?** SafetyCulture has helped manufacturing businesses around the world to **reduce reporting time by 60%**. Find out more about how we can help your manufacturing business.

Even though these cybersecurity risks can seem daunting, overcoming them is well within your control. If you stay aware and cautious, you can keep your workplace and people safe.

Cybersecurity tips for manufacturing workers

If you want to keep your workplace secure from credential stuffing, supply chain attacks, phishing, ransomware, and internal breaches, keep these tips in mind.

1. Create strong passwords

As tempting as it is to go with easy-to-remember ‘password1’, it’s best to rethink that strategy. Many manufacturers have experienced cyber attacks because of weak login credentials. For example, software manufacturer SolarWinds was publicly embarrassed when a security professional discovered the password ‘solarwinds123’ allowed access

to its server. The company later experienced a supply chain attack that impacted more than 18,000 clients.

For context, a 12-character password with one symbol, number, and uppercase letter would take a computer 34,000 years to hack. Even better – consider investing in secure password management tools for your business.

“It would be helpful for businesses to consider using a password manager to both generate and store their passwords,” Steven says. “They should aim to have unique passwords for all logins and avoid password reuse.”

2. Enable multi-factor authentication

Fortunately, multi-factor authentication can protect you even if your login details get leaked or stolen. Upon signing in, it will ask you to confirm your activity via an app, phone number, or email. This way, you can keep hackers at bay even if they know your password. Best of all, it notifies you whenever there’s a new sign-in attempt, so you’re able to confirm or deny this action.

> **Did you know?** The SafetyCulture platform enables you to set up your login via Single Sign On (SSO), which protects you from things like weak or leaked passwords.

3. Brush up on training

You may have run cybersecurity training for your team already, but it’s best practice to do this regularly. Workers forget 50% of the training material after a few days.

SafetyCulture Training has more than 1,000 mobile-led training courses. You’ll see much faster improvements if you enable reminders for your online sessions and make learning a routine.

4. Create backups

During a ransomware attack, a backup is your best line of defense – especially considering manufacturing has the lowest chance of data recovery out of every

industry. Having copies means you won't be vulnerable to ransom – you'd simply wipe your company devices, remove the malware, and start over. Already, 73% of manufacturing facilities use backups instead of paying.

Backups are essential because cybercriminals don't always honor their promises. For example, a UK manufacturer paid a $3 million ransom only to experience a second ransomware attack from the same hackers a month later. If your company pays up, there's no guarantee you won't get hit again.

> **Check it out:** The proof is in the production line. Read the success stories of our manufacturing customers who've used the SafetyCulture platform to improve their workplace operations.

5. Report suspicious behavior

Typically, only management can enforce security standards on third-party vendors. Still, your employees can do their part if they notice suspicious behavior or unsafe practices. SafetyCulture's Issues feature can be used to instantly report cybersecurity incidents using the QR code capabilities. Since it lets you attach pictures, videos, or your location, you can get your IT team up to date within minutes. Manufacturing companies can request security, privacy and/or compliance documentation from third parties to evaluate how secure they are as well.

Safeguarding manufacturing from cyber threats

If you keep the manufacturing industry's biggest threats in mind whenever you deal with devices or software, you can protect your workplace. Following the best practices and helpful tips does a lot to safeguard against malware and data breaches.

Dive into more industry-related articles on our blog:

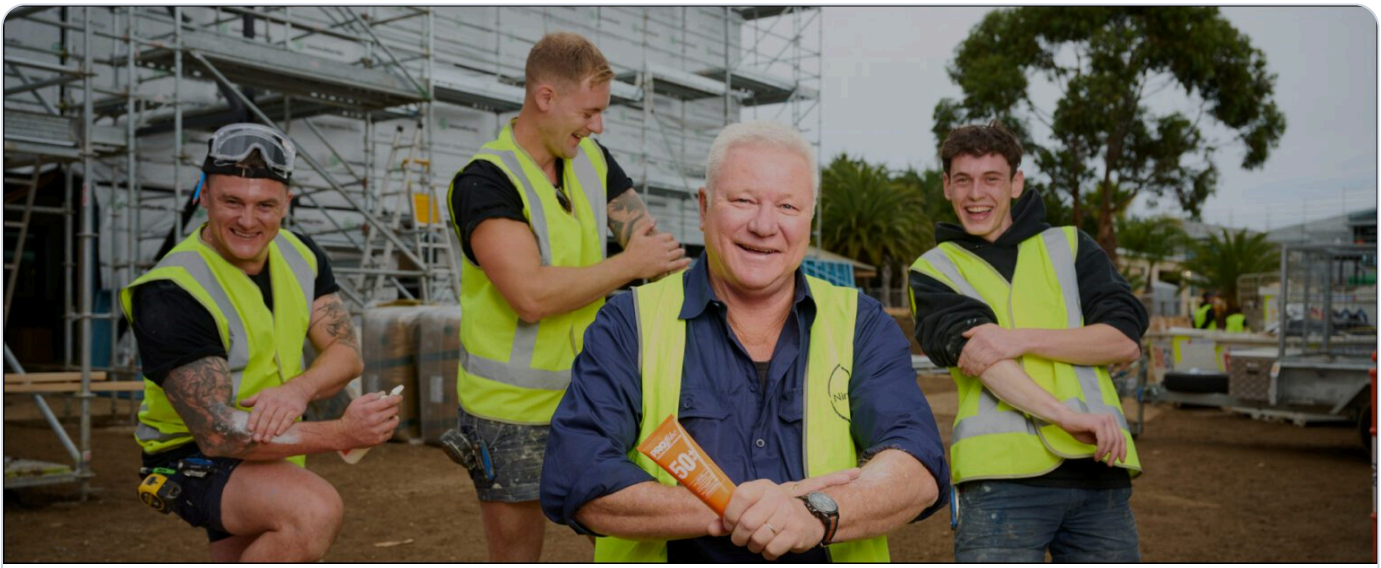
- How does a fire prevention plan benefit your workplace?
- Top 10 best work gear you need on SafetyCulture Marketplace
- Personal safety tips to keep lone workers safe

Like this article? Why not share it!

Important Notice

The information contained in this article is general in nature and you should consider whether the information is appropriate to your specific needs. Legal and other matters referred to in this article are based on our interpretation of laws existing at the time and should not be relied on in place of professional advice. We are not responsible for the content of any site owned by a third party that may be linked to this article. SafetyCulture disclaims all liability (except for any liability which by law cannot be excluded) for any error, inaccuracy, or omission from the information contained in this article, any site linked to this article, and any loss or damage suffered by any person directly or indirectly through relying on this information.

Related articles

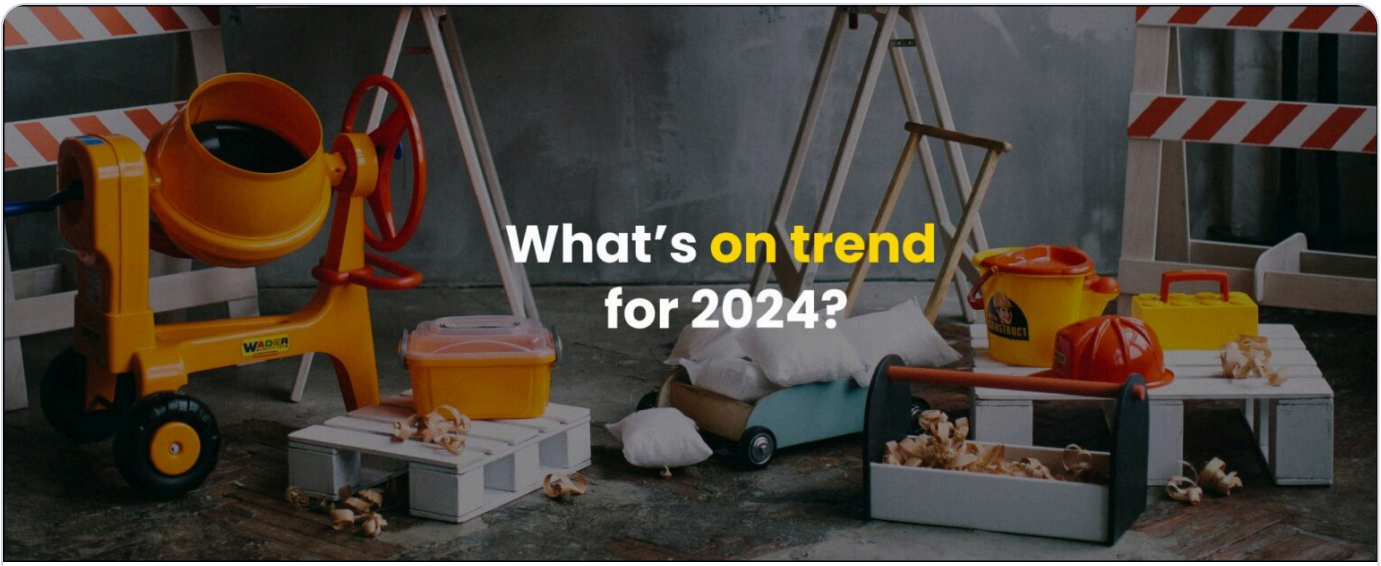


Industry Trends | World Of Work

Changing attitudes on the frontline: Sun protection for outdoor workers

By SafetyCulture Team

Read this post →



Industry Trends

Top environmental, health and safety (EHS) trends for 2024

By SafetyCulture Team

Read this post →

Industry Trends

Top 10 best work gear you need on SafetyCulture Marketplace

By SafetyCulture Team

Read this post →

SafetyCulture

Product

Inspection Software

Temperature logging

SafetyDocs

Checklist App

Checklist Maker

Resources

Templates

Checklists

Topics

Blog

Events & Webinars

Apps

API

Support

Support center

Product updates

Book a demo

Integrations

Company

About us

Careers

Meet the team

Contact us

Status
Privacy
Terms & conditions
Security

© The Loop by Safetyculture 2024